Deepfakes now 2nd most common cybersecurity incident for US businesses, according to ISMS.online research

Deepfakes now 2nd most common cybersecurity incident for US businesses, according to ISMS.online research; Have been experienced by over 1/3 of organizations

NEW YORK, NEW YORK, USA, May 20, 2024 /EINPresswire.com/ -- Deepfakes are now the second most common cybersecurity incident encountered by businesses in the past year, trailing only behind malware infections, according to research by ISMS.online, the auditor approved compliance platform. Astonishingly over a third of businesses across the US have experienced a deepfake security incident in the last 12 months.

> It is deeply concerning to see the number of organizations threatened by both deep fake and third-party vendor risks"
>
> *Luke Dash, CEO, ISMS.online*

ISMS.online's 'State of Information Security' report surveyed 518 people in the US who work in information security across 10 sectors including technology, manufacturing, education, energy and utilities and healthcare.

Key findings include:

• 35% of US businesses have experienced a deepfake security incident in the last 12 months, ranking the second most common cybersecurity incident in the country.

• 37% of US businesses state that managing third party vendor risk is the biggest data security challenge they currently face, with 43% citing that partner data has been the most compromised in the last 12 months.

• More than a third (39%) said financial allocations for securing supply chain and third-party vendor connections are set to increase by up to 25% in the coming year.

• Nearly three quarters (73%) of US respondents think that AI and ML are improving cybersecurity, though only 26% have adopted initiatives using these new technologies over the past 12 months. Additionally, 25% cite that managing and securing emerging technology like AI and ML is a challenge.

The most likely scenario today for threat actors to use deepfakes is in business email compromise (BEC)-style attempts. Attackers use the AI-powered voice and video-cloning technology to trick recipients into making corporate fund transfers. However, there are possible use cases for information/credential theft, reputational damage or even to bypass facial and voice recognition authentication. And with partner data (43%) being cited as the most compromised in the past 12 months by US respondents, more businesses need to be vigilant when it comes to the risks posed by their third-party vendors and suppliers, especially in light of these new, sophisticated attacks.

Luke Dash, CEO of ISMS.online commented, “It is deeply concerning to see the number of organizations threatened by both deep fake and third-party vendor risks. To address these rising and more sophisticated threats, organizations must continue to build robust and effective cybersecurity foundations, especially as advanced technology like AI and ML is available to help support data security initiatives.”

American respondents are adopting AI and ML technologies to thwart threats, though they are still in the early stages. Only a quarter (26%) have put initiatives in place in the past 12 months, though a much larger majority (73%) agree that AI and ML will help to improve data security programs. Despite the positive attitudes toward AI and ML, 25% of respondents list managing and securing emerging tech like AI, ML and blockchain as a top challenge and only about a third (36%) intend to increase cybersecurity spend by up to 25% in the next 12 months.

Dash continued, “It’s still unclear how new, advanced technologies like AI and ML are going to change the data security landscape. We are certain, however, that governments across the globe will push for more, not less, regulation. Standards like ISO 42001, which deals with AI, will help organizations provide assurances to partners, customers and regulators. Having these in place are truly essential to building a better business, longevity and financial success.”

-ends-

About ISMS.online
ISMS.online is revolutionizing the way businesses across the globe handle data privacy and information security compliance. The cutting-edge SaaS platform provides a comprehensive roadmap to robust and scalable governance, risk and compliance for organizations of all sizes and maturities. With a global presence and over 25,000 users, including enterprise clients like Moneycorp, Siemens and Ricoh, ISMS.online simplifies complex processes across over 100 standards and regulations, empowering organizations worldwide to secure and scale their compliance with ease.

Research Methodology
ISMS.online commissioned leading independent market research firm Censuswide conducted the research. With a sample of 1,526 respondents who work in information security across the

UK (502), USA (518) and Australia (506), the research uncovers the main information security and compliance challenges facing organizations in these regions. The survey fieldwork took place between 03.22.2024 – 04.02.2024.

Sarah Hawley
Origin Communications
+1 480-292-4640
email us here
